

Unit-4

Network Layer

PREPARED BY: SUSHANT BHATTARAI

Functions of Network Layer

2

- ▶ Logical Addressing
- ▶ Routing
- ▶ Fragmenting
- ▶ Packeting

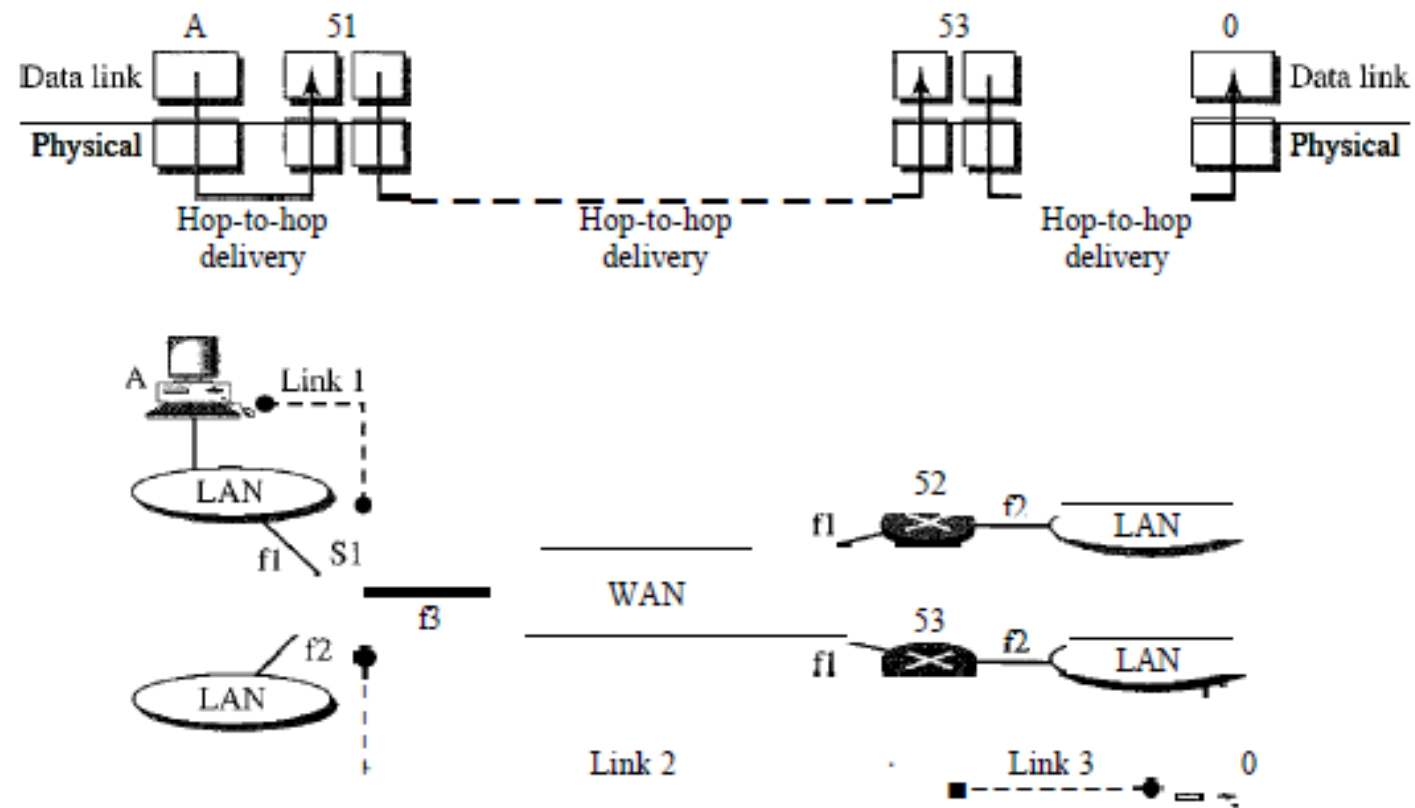
Internetworking

- ▶ The physical and data link layers of a network operate locally. These two layers are jointly responsible for data delivery on the network from one node to the next, as shown in Figure below.
- ▶ This internetwork is made of five networks: four LANs and one WAN. If host A needs to send a data packet to host D, the packet needs to go first from A to R1 (a switch or router), then from R1 to R3, and finally from R3 to host D.
- ▶ We say that the data packet passes through three links. In each link, two physical and two data link layers are involved.

Internetworking

4

Figure 20.1 *Links between two hosts*



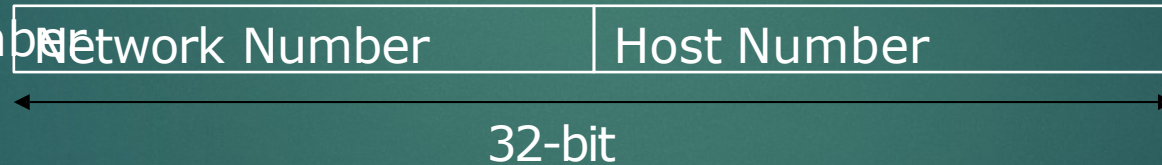
IPV4 Addressing

3

- ▶ 32 bit
- ▶ Displayed in dotted decimal notation
- ▶ Uses two level of hierarchical addressing

- ▶ Network Number

- ▶ Host Number



- ▶ Network Number is assigned by Internet Network Information Centre(InterNIC) if the network is the part of public network

IPV4 Classful Addressing

- ▶ Consist of 2^{32} address
- ▶ In order to support network of different sizes it is divided into different class
- ▶ Must be kept in mind this classification is applicable to internet only
- ▶ A private network can have its own address structure
- ▶ There are 5 different categories or classes of IP addresses
- ▶ Originally there were only 3 categories of IP address

Categories of IP Address

- ▶ Class A
- ▶ Class B
- ▶ Class C
- ▶ Class
D
- ▶ Class E

Class A address

8

- ▶ Consist of large number of hosts
- ▶ Network ID is 8-bit long
- ▶ Host ID is 24 bit long
- ▶ The MSB of this class IP address is always set to zero(0).
- ▶ The remaining 7 bit in first octet are used to determine network ID.
- ▶ Remaining 24 bits of host ID are used to determine the host in any network

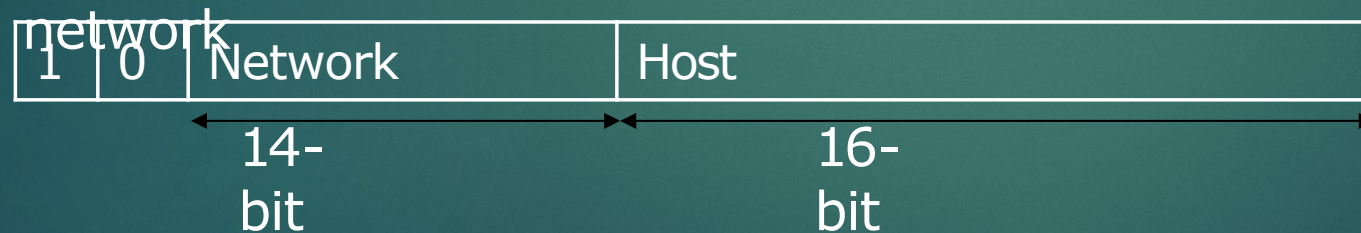


Class A address

- ▶ Class A IP address ranges from 1-127(00000001-01111111)
- ▶ It includes only IP starting from 1.X.X.X-126.X.X.X only.
- ▶ The IP range 127.X.X.X is reserved for loopback IP address
- ▶ Default subnet mask of class A IP address is 255.0.0.0

Class B address

- ▶ Network ID is 14-bit long
- ▶ Host ID is 16 bit long
- ▶ The first two bit of this class IP address is always set to 10.
- ▶ The remaining 14 bit are used to determine network ID.
- ▶ Remaining 16 bits of host ID are used to determine the host in any



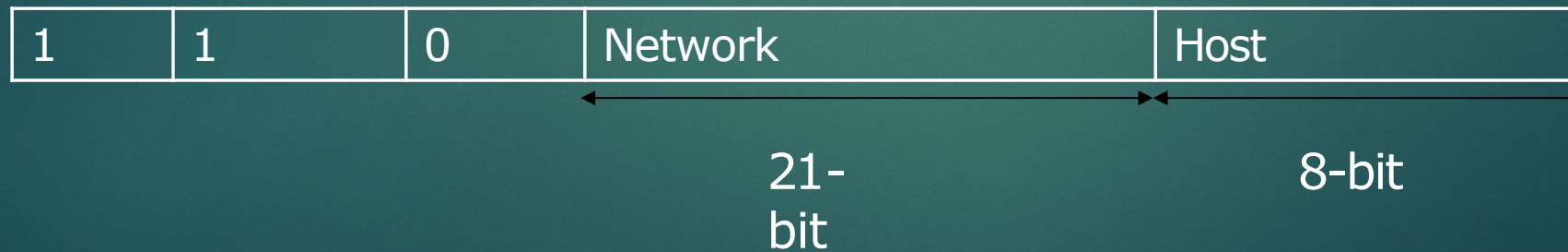
Class B address

- ▶ Class B IP address ranges from 128-191(10000001-10111111)
- ▶ It includes only IP starting from 128.0.X.X-191.255.X.X only.
- ▶ Default subnet mask of class B IP address is 255.255.0.0

Class C address

12
0

- ▶ Network ID is 24-bit long
- ▶ Host ID is 8 bit long
- ▶ The first three bit of this class IP address is always set to 110.
- ▶ The remaining 21 bit are used to determine network ID.
- ▶ Remaining 8 bits of host ID are used to determine the host in any network



Class C Address

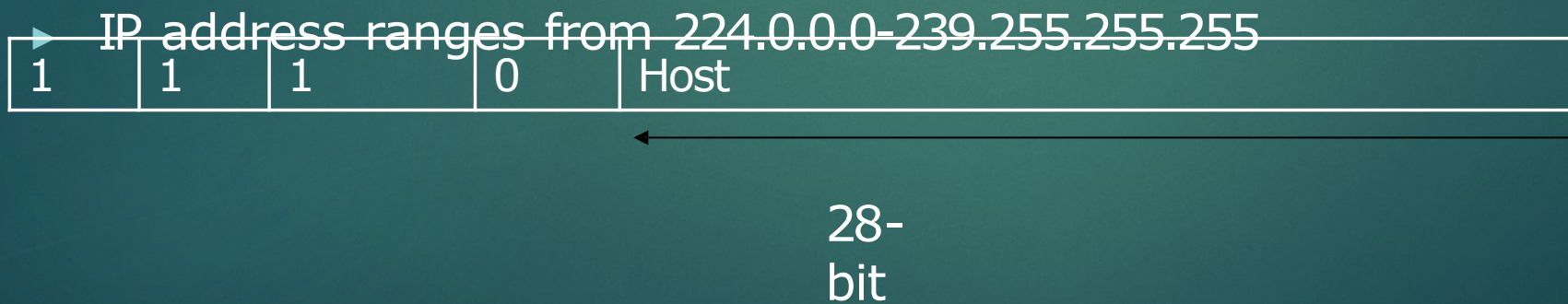
13
1

- ▶ Class C IP address ranges from 192-223(10000001-10111111)
- ▶ It includes only IP starting from 192.0.0.X-223.255.255.X only.
- ▶ Default subnet mask of class C IP address is 255.255.255.0

Class D address

14
2

- ▶ Reserved for multicasting
- ▶ The first four bit of this class IP address is always set to 1110.
- ▶ The remaining bit are used for the address that interested host recognize.
- ▶ This class lacks subnet mask



Class E address

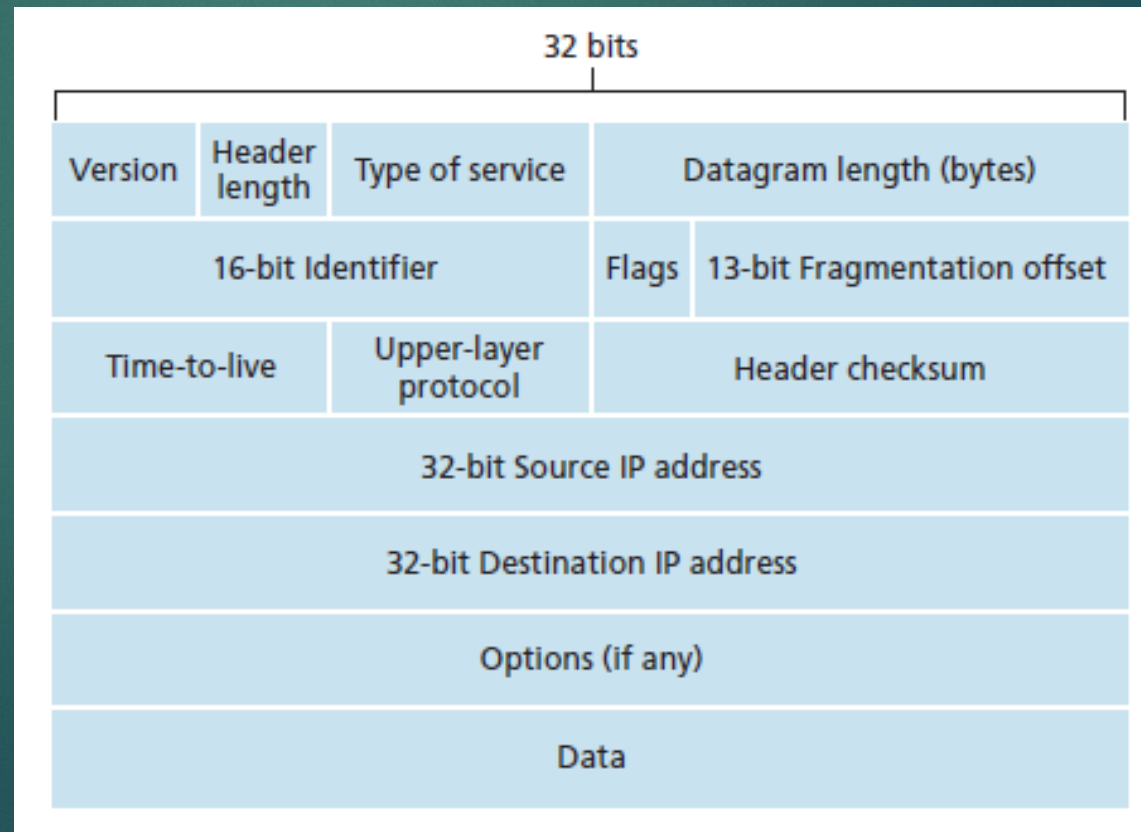
15
3

- ▶ Reserved for experimental and research purpose
- ▶ The first four bit of this class IP address is always set to 1111.
- ▶ The remaining bit are used for the address that interested host recognize.
- ▶ This class lacks subnet mask
- ▶ IP address ranges from 240.0.0.0-255.255.255.255

IPv4 datagram format

16
5

- ▶ Internet Protocol being a layer-3 protocol (OSI) takes data Segments from layer-4 (Transport) and divides it into packets. IP packet encapsulates data unit received from above layer and add to its own header information



IPv4 datagram format

17
6

- ▶ Version: Version no. of Internet Protocol used (e.g. IPv4).
- ▶ IHL: Internet Header Length; Length of entire IP header.
- ▶ Service type
- ▶ DSCP: Differentiated Services Code Point; this is Type of Service.
- ▶ ECN: Explicit Congestion Notification; It carries information about the congestion seen in the route.
- ▶ Total Length: Length of entire IP Packet (including IP header and IP Payload).
- ▶ Identification: If IP packet is fragmented during the transmission, all the fragments contain same identification number to identify original IP packet they belong to.
- ▶ Flags: As required by the network resources, if IP Packet is too large to handle, these 'flags' tells if they can be fragmented or not. In this 3-bit flag, the MSB is always set to '0'.
- ▶ Fragment Offset: This offset tells the exact position of the fragment in the original IP Packet.

IPv4 datagram format

18
7

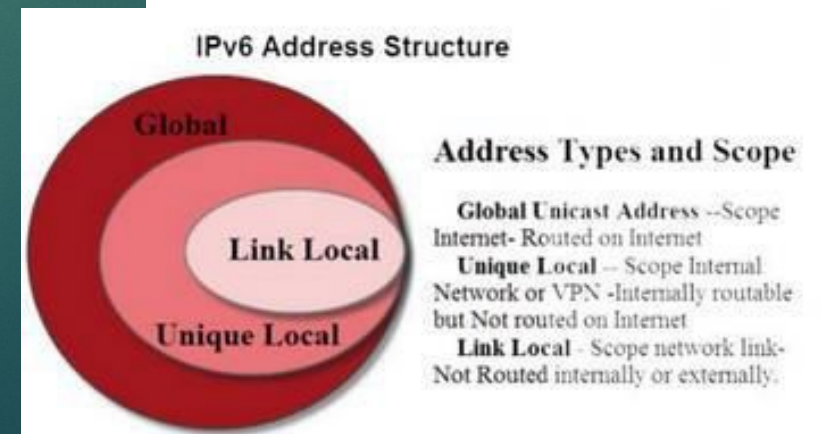
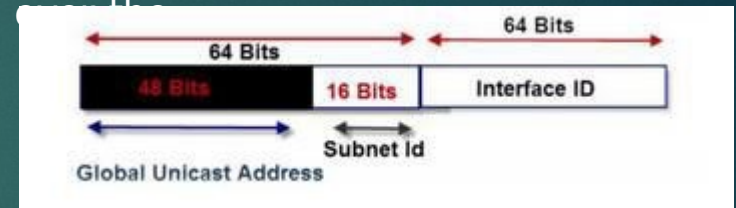
- ▶ Time to Live: To avoid looping in the network, every packet is sent with some TTL value set, which tells the network how many routers (hops) this packet can cross.
- ▶ At each hop, its value is decremented by one and when the value reaches zero, the packet is discarded.
- ▶ Protocol: Tells the Network layer at the destination host, to which Protocol this packet belongs to, i.e. the next level Protocol. For example protocol number of ICMP is 1, TCP is 6 and UDP is 17.
- ▶ Header Checksum: This field is used to keep checksum value of entire header which is then used to check if the packet is received error-free.
- ▶ Source Address: 32-bit address of the Sender (or source) of the packet.
- ▶ Destination Address: 32-bit address of the Receiver (or destination) of the packet.
- ▶ Options: This is optional field, which is used if the value of IHL is greater than 5. These options may contain values for options such as Security, Record Route, Time Stamp, etc.

- ▶ A new Internet addressing system Internet Protocol version 6 (IPv6) is being deployed to fulfill the need for more Internet addresses.
- ▶ IPv6 (Internet Protocol Version 6) is also called IPng (Internet Protocol next generation) and it is the newest version of the Internet Protocol (IP) reviewed in the IETF (Internet Engineering Task Force) standards committees to replace the current version of IPv4 (Internet Protocol Version 4).
- ▶ IPv6 is the successor to Internet Protocol Version 4 (IPv4). It was designed as an evolutionary upgrade to the Internet Protocol and will, in fact, coexist with the older IPv4 for some time.
- ▶ IPv6 is designed to allow the Internet to grow steadily, both in terms of the number of hosts connected and the total amount of data traffic transmitted.
- ▶ An IPv6 address consists of eight groups of four hexadecimal digits. If a group consists of four zeros, the notation can be shortened using a colon to replace the zeros.
- ▶ IP v6 was developed by Internet Engineering Task Force (IETF) to deal with the problem of IPv4 exhaustion. IP v6 is 128-bits address having an address space of 2^{128} , which is way bigger than IPv4. In IPv6 we use Colon-Hexa representation.
- ▶ There are 8 groups and each group represents 2 Bytes and separated by colon.

IPv6

20
9

- ▶ For Network And Node Addresses The first step is to split the address into two parts.
- ▶ The upper 64 bits are used for routing.
- ▶ the address is split into 2 64 bit segments the top 64 bits is the network part and the lower 64 bits the node part:
- ▶ The lower 64 bits identify the address of the interface or node, and is derived from the actual physical or MAC address using IEEE's Extended Unique Identifier (EUI-64) format.
- ▶ If we look at the upper 64 bits in more detail we can see that it is split into 2 blocks of 48 and 16 bits respectively the lower 16 bits are used for subnets on an internal networks, and are controlled by a network administrator.
- ▶ The upper 48 bits are used for the global network addresses and are for routing on the internet.
- ▶ Address Types and Scope
- ▶ IPv6 addresses have three types:
- ▶ Global Unicast Address –Scope Internet- routed on Internet
- ▶ Unique Local — Scope Internal Network or VPN internally routable, but Not routed on Internet
- ▶ Link Local – Scope network link- Not Routed internally or externally.



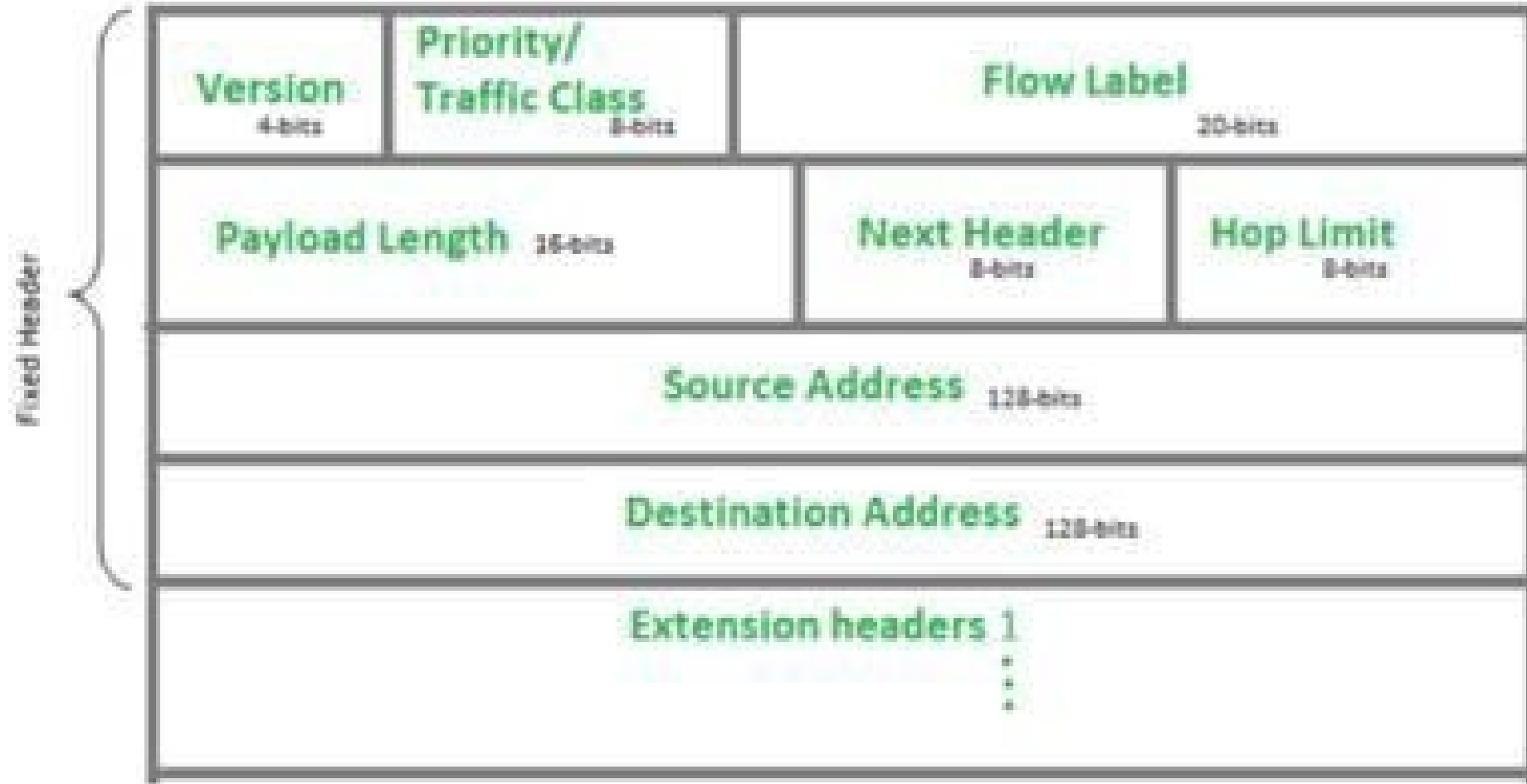
Benefit of IPV6

21
0

- ▶ No more NAT (Network Address Translation)
- ▶ Auto-configuration
- ▶ No more private address collisions
- ▶ Better multicast routing
- ▶ Simpler header format
- ▶ Simplified, more efficient routing
- ▶ True quality of service (QoS), also called "flow labeling"
- ▶ Built-in authentication and privacy support
- ▶ Flexible options and extensions

IPv6 datagram format

22
1



IPv6 datagram format

- ▶ Version (4-bits) : Indicates version of Internet Protocol which contains bit sequence 0110.
- ▶ Traffic Class (8-bits) : The Traffic Class field indicates class or priority of IPv6 packet which is similar to Service Field in IPv4 packet. It helps routers to handle the traffic based on priority of the packet. If congestion occurs on router then packets with least priority will be discarded
- ▶ Flow Label (20-bits) : This field was added in IPv6 to differentiate traffic. A flow label and source IP address identify a data flow. Intermediate network devices can effectively differentiate data flows based on this field., such as non-default quality of service or real time service.
- ▶ Payload Length (16-bits) : It is a 16-bit (unsigned integer) field, indicates total size of the payload which tells routers about amount of information a particular packet contains in its payload

IPv6 datagram format

24
3

- ▶ Next Header (8-bits) : Next Header indicates type of extension header(if present) immediately following the IPv6 header. Whereas In some cases it indicates the protocols contained within upper- layer packet, such as TCP, UDP.
- ▶ Hop Limit (8-bits) : Hop Limit field is same as TTL(Time to Leave) in IPv4 packets. It indicates the maximum number of intermediate nodes IPv6 packet is allowed to travel.
- ▶ Source Address (128-bits) : Source Address is 128-bit IPv6 address of the original source of the packet.
- ▶ Destination Address (128-bits) : Destination Address field indicates the IPv6 address of the final destination(in most cases). All the intermediate nodes can use this information in order to correctly route the packet.

Advantage

S

25
4

- ▶ **More Efficient Routing:** IPv6 reduces the size of routing tables and makes routing more efficient and hierarchical
- ▶ **More Efficient Packet Processing:** IPv6's simplified packet header makes packet processing more efficient. IPv6 contains no IP-level checksum, so the checksum does not need to be recalculated at every router hop
- ▶ **Directed Data Flows:** IPv6 supports multicast rather than broadcast. Multicast allows bandwidth-intensive packet flows (like multimedia streams) to be sent to multiple destinations simultaneously, saving network bandwidth
- ▶ **Simplified Network Configuration:** Address auto-configuration (address assignment) is built in to IPv6. A host can generate its own IP address by appending its link-layer (MAC) address, converted into Extended Universal Identifier (EUI) 64-bit format, to the 64 bits of the local link prefix.
- ▶ **Support For New Services:** By eliminating Network Address Translation (NAT), true end-to-end connectivity at the IP layer is restored, enabling new and valuable services
- ▶ **Security:** IPSec, which provides confidentiality, authentication and data integrity, is baked into IPv6
- ▶ **Smaller routing table:** only a single optimal route for each network id is stored in the routing table.
- ▶ **Low network overhead:** Do not exchange any routing information when the internetwork has Scale well to large and very large internetwork

Assignment

226
5

- ▶ List down the disadvantages of IPV6

IPv4

IPv6

The Address Space is 32 bits.	The space is 128 bits.
The length of header is 20 bytes	The length of header is 40
4 bytes for each address in the header	16 bytes for each address in the header
The number of Header field 12	The number of header field 8
Checksum field, used to measure error in the header, required	Checksum field eliminated from header as error in the IP header are not very crucial
Internet Protocol Security (IPSec) with respect to network security is optional	Internet Protocol Security (IPSec) With respect to network security is mandatory
No identification to the packet flow (Lack of QoS handling).	The flow level field on the header portion identifies the packet flow and directs to router (Efficient QoS handling)
The Fragmentation is done both by sending host and routers	The fragmentation is done both by sending host; there is no role of the routers.
No identification to the packet flow (Lack of QoS handling).	The flow level field on the header portion identifies the packet flow and directs to router (Efficient QoS handling)
Clients have approach Dynamic Host Configuration server (DHCP) whenever they connect to a network.	Clients do not have to approach any such server as they are given permanent addresses.

Forwarding

28

- ▶ Forwarding means to place the packet in its route to its destination. Forwarding requires a host or a router to have a routing table.
- ▶ When a host has a packet to send or when a router has received a packet to be forwarded, it looks at this table to find the route to the final destination.
- ▶ Forwarding Techniques
- ▶ Several techniques can make the size of the routing table manageable and also handle issues such as security
 - ▶ Next hop v/s Route method
 - ▶ Network Specific v/s Host specific method

Next hop v/s Route method

29

- ▶ One technique to reduce the contents of a routing table is called the next-hop method.
- ▶ In this technique, the routing table holds only the address of the next hop instead of information about the complete route (route method).
- ▶ The entries of a routing table must be consistent with one another

Next hop v/s Route method

30

Figure 22.2 *Route method versus next-hop method*

a. Routing tables based on route

Destination	Route
HostB	R1, R2, host B

Routing table
for host A

Destination	Route
HostB	R2, host B

Routing table
for R1

Destination	Route
HostB	HostB

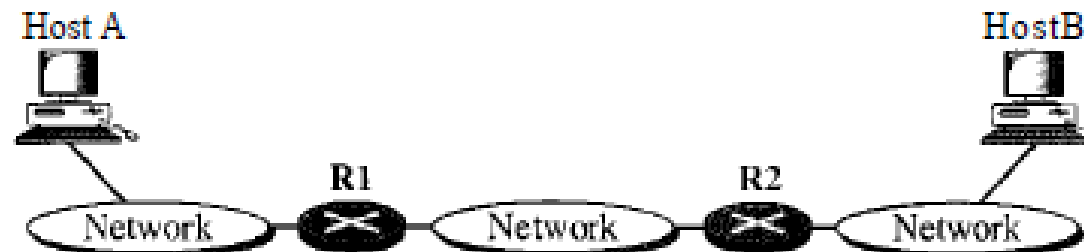
Routing table
for R2

b. Routing tables based on next hop

Destination	Next hop
Host B	R1

Destination	Next hop
HostB	R2

Destination	Next hop
Host B	



Network Specific v/s Host specific method

31

- ▶ A second technique to reduce the routing table and simplify the searching process is called the network-specific method.
- ▶ Instead of having an entry for every destination host connected to the same physical network (host-specific method), we have only one entry that defines the address of the destination network itself.
- ▶ In other words, we treat all hosts connected to the same network as one single entity. For example, if 1000 hosts are attached to the same network, only one entry exists in the routing table instead of 1000

Network Specific v/s Host specific method

32

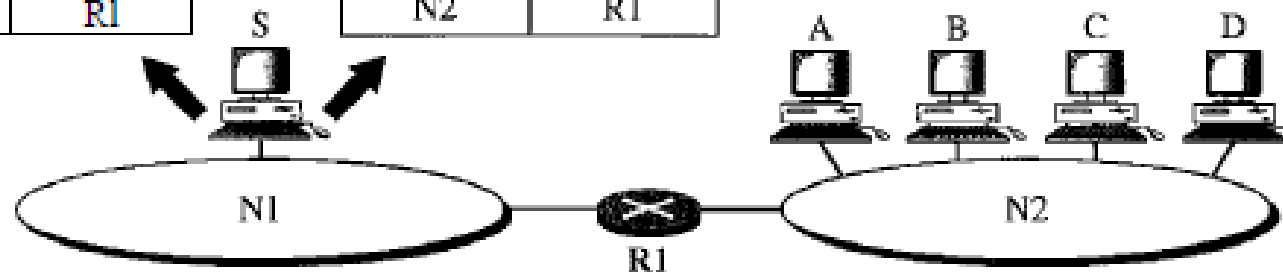
Figure 22.3 *Host-specific versus network-specific method*

Routing table for host S based
on host-specific method

Destination	Next hop
A	R1
B	R1
C	R1
D	R1

Routing table for host S based
on network-specific method

Destination	Next hop
N2	R1



Routing

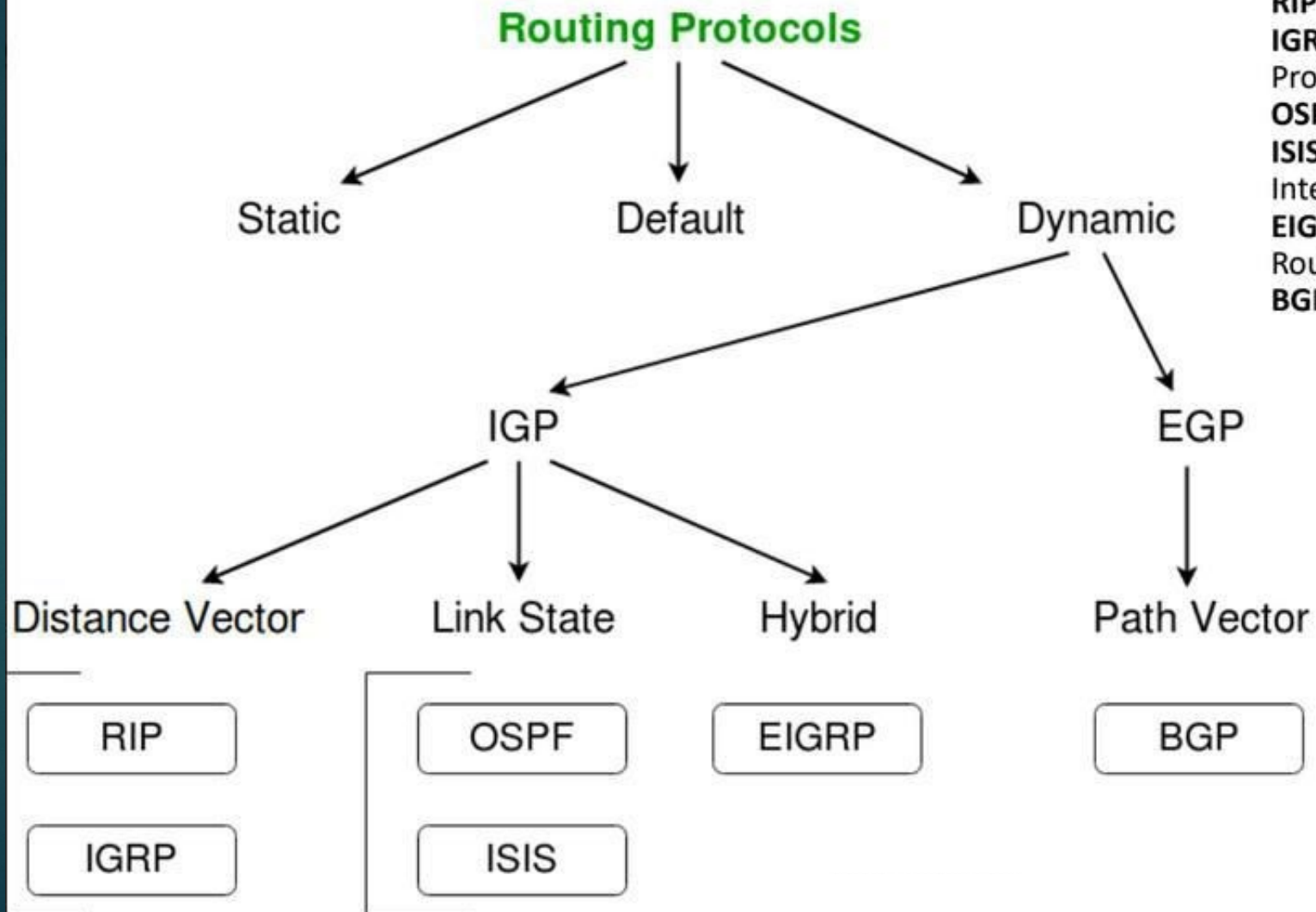
23
8

- ▶ routing is the process of selecting a path across one or more networks
- ▶ An IP datagram is routed hop-by-hop across a network to the destination using forwarding tables that are stored in the routers in advance
- ▶ When an IP packet is received by a router, its Destination Address (DA) is matched with one of the entries in the forwarding table and the IP packet is forwarded through the interface indicated in the forwarding table

Types of Routing

34

Routing Algorithm:



- **IGP** – Interior Gateway Protocol
- EGP** – Exterior Gateway Protocol
- RIP** – Routing Information Protocol
- IGRP** – Interior Gateway Routing Protocol
- OSPF** – Open Shortest Path First
- ISIS** – Intermediate System to Intermediate System
- EIGRP** – Enhanced Interior Gateway Routing Protocol
- BGP** – Border Gateway Protocol

Static Routing

35
0

- ▶ Static routing is a process in which we have to manually add routes in routing table.
- ▶ the routing decision is not based on the measurement or estimations of current traffic and topology.
- ▶ It is a technique in which the administrator manually adds the routes in a routing table.
- ▶ A Router can send the packets for the destination along the route defined by the administrator.
- ▶ In this technique, routing decisions are not made based on the condition or topology of the networks

Advantage s

36
1

- ▶ No routing overhead for router CPU which means a cheaper router can be used to do routing.
- ▶ It adds security because only administrator can allow routing to particular networks only.
- ▶ No bandwidth usage between routers.

Dis-advantages

37
2

- ▶ For a large network, it is a hectic task for administrator to manually add each route for the network in the routing table on each router.
- ▶ The administrator should have good knowledge of the topology.
- ▶ If a new administrator comes, then he has to manually add each route so he should have very good knowledge of the routes of the topology.

Dynamic Routing(adaptive)

38
3

- ▶ Dynamic routing makes automatic adjustment of the routes according to the current state of the route in the routing table.
- ▶ Dynamic routing uses protocols to discover network destinations and the routes to reach it. RIP and OSPF are the best examples of dynamic routing protocol.
- ▶ Automatic adjustment will be made to reach the network destination if one route goes down.
- ▶ Routers exchange routing information when there is a topology change. This exchange allows routers to automatically learn about new networks and also to find alternate paths when there is a link failure to a current network..
- ▶ When a router finds a change in the topology then router advertises it to all other routers network.

Advantage

S

- ▶ Easy to configure.
- ▶ More effective at selecting the best route to a destination remote network and also for discovering remote

Disadvantages

30
5

- ▶ Consumes more bandwidth for communicating with other neighbors.
- ▶ Less secure than static routing

Basis Of Comparison		
	Adaptive Routing algorithm	Non-Adaptive Routing algorithm
Define	Adaptive Routing algorithm is an algorithm that constructs the routing table based on the network conditions.	The Non-Adaptive Routing algorithm is an algorithm that constructs the static table to determine which node to send the packet.
Usage	Adaptive routing algorithm is used by dynamic routing.	The Non-Adaptive Routing algorithm is used by static routing.
Routing decision	Routing decisions are made based on topology and network traffic.	Routing decisions are the static tables.
Categorization	The types of adaptive routing algorithm, are Centralized, isolation and distributed algorithm.	The types of Non Adaptive routing algorithm are flooding and random walks.
Complexity	Adaptive Routing algorithms are more complex.	Non-Adaptive Routing algorithms are simple.

Distance Vector Algorithm

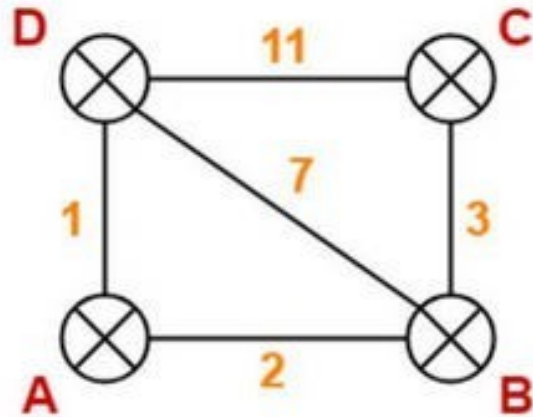
32
7

- ▶ As from the name suggests it uses distance and direction to find the best path to reach the destination.
- ▶ The distance here is the number of hops a packet crosses to reach the destination. Each hop refers to a router across the path.
- ▶ The word vector refers to the direction of the packet to reach the destination. It has lesser convergence time and knowledge about the whole network when compared to link state routing algorithm.
- ▶ Working mechanism:
 - ▶ Step 1: In this algorithm, the information about every router connected directly and routing updates will be gathered by every single router.
 - ▶ each router prepares its routing table by their local knowledge each router knows about
 - ▶ All the routers present in the network.
 - ▶ Distance to its neighboring router..

Distance Vector Algorithm

33
8

- ▶ Step 2:
 - ▶ All the information collected by a single router about the whole network will be sent only to its neighbors and not to all other routers in the routing table.
 - ▶ If there is any change in the hop count or disabled paths it will be updated only to its neighbors which in turn after a period passes to its neighbors.
- ▶ Step 3:
 - ▶ The above explained sharing of information will take place in a period of 30 seconds.
 - ▶ If there is a change in the network like if a network fails or additionally a router is added to the network, the changed information will be updated only after that time period



At Router A-

Destination	Distance	Next Hop
A	0	A
B	2	B
C	∞	—
D	1	D

At Router B-

Destination	Distance	Next Hop
A	2	A
B	0	B
C	3	C
D	7	D

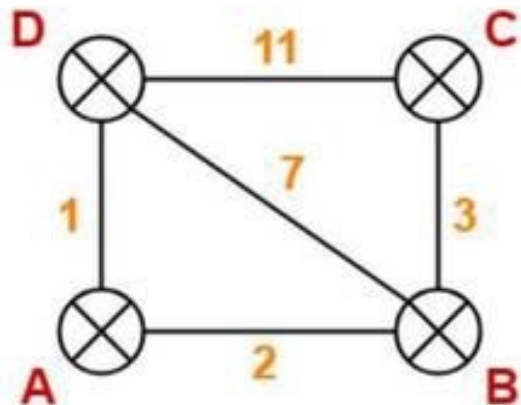
At Router C-

Destination	Distance	Next Hop
A	∞	—
B	3	B
C	0	C
D	11	D

At Router D-

Destination	Distance	Next Hop
A	1	A
B	7	B
C	11	C
D	0	D

- Router B receives distance vectors from its neighbors A, C and D
- Router B prepares a new routing table as.



- Router B prepares a new routing table as-

From A	From C	From D	
0	∞	1	
2	3	7	
∞	0	11	
1	11	0	
Cost (B→A) = 2 Cost (B→C) = 3 Cost (B→D) = 7			

Destination	Distance	Next hop
A		
B	0	B
C		
D		

New Routing Table at Router B

- Cost of reaching destination A from router B = $\min \{ 2+0, 3+\infty, 7+1 \} = 2$ via A.
- Cost of reaching destination C from router B = $\min \{ 2+\infty, 3+0, 7+11 \} = 3$ via C.
- Cost of reaching destination D from router B = $\min \{ 2+1, 3+11, 7+0 \} = 3$ via A.

Thus, the new routing table at router B is-

Destination	Distance	Next Hop
A	2	A
B	0	B
C	3	C
D	3	A

Routing Information Protocol(RIP)

46
1

- ▶ Routing Information Protocol (RIP) is a dynamic routing protocol which uses hop count as a routing metric to find the best path between the source and the destination network.
- ▶ It is a distance vector routing protocol which has AD value 120 .RIP uses port number 520.
- ▶ It faces a problem of Slow convergence. Whenever the router or link fails, then it often takes minutes to stabilize or take an alternative route; This problem is known as Slow convergence
- ▶ sends routing information updates every 30 seconds(Update timer), which is termed advertising. If a device does not receive an update from another device for 180 seconds or more(hold down timer), the receiving device marks the routes served by the non updating device as unusable. If there is still no update after 240 seconds(flush timer), the device removes all routing table entries for the non updating device.

- ▶ Hop Count :
- ▶ Hop count is the number of routers occurring in between the source and destination network. The path with the lowest hop count is considered as the best route to reach a network and therefore placed in the routing table.
- ▶ RIP prevents routing loops by limiting the number of hops allowed in a path from source and destination. The maximum hop count allowed for RIP is 15 and hop count of 16 is considered as network unreachable
- ▶ Two type of RIP are:
- ▶ RIP v1 is known as Classful Routing Protocol because it doesn't send information of subnet mask in its routing update.
- ▶ uses broadcast UDP data packets, to exchange the routing information.
- ▶ RIP v2 is known as Classless Routing Protocol because it sends information of subnet mask in its routing update.
- ▶ RIPv2 uses multicast packets to exchange the routing information.

Working Principle

48
3

- ▶ RIP uses a distance vector algorithm to decide which path to put a packet on to get to its destination.
- ▶ Each router broadcasts its entire routing table to its closest neighbors every 30 sec. In this context, neighbors are the other routers to which a router is connected directly, that is, the other routers on the same network segments as the selected router.
- ▶ The neighbors, in turn, pass the information on to their nearest neighbors, and so on, until all RIP hosts within the network have the same knowledge of routing paths. This shared knowledge is known as convergence.
- ▶ If a router receives an update on a route, and the new path is shorter, it will update its table entry with the length and next-hop address of the shorter path.
- ▶ If the new path is longer, it will wait through a "hold-down" period to see if later updates reflect the higher value as well. It will only update the table entry if the new, longer path has been determined to be stable.
- ▶ If a router crashes or a network connection is severed, the network discovers this because that router stops sending updates to its neighbors, or stops sending and receiving updates along the severed connection.
- ▶ If a given route in the routing table isn't updated across six successive update cycles (that is, for 180 seconds) a RIP router will drop that route and let the rest of the network know about the problem through its own periodic updates.

Features of RIP

49
4

- ▶ Updates of the network are exchanged periodically.
- ▶ Updates (routing information) are always broadcast.
- ▶ Full routing tables are sent in updates.
- ▶ Routers always trust on routing information received from neighbor routers. This is also known as Routing on rumors.

Link state protocol

40
5

1. Each router is responsible for meeting its neighbors and learning their names.
 - Used a **Hello Protocol**, which send a data packet contains RID and address of the network on which the packet is being sent
2. Each router constructs a **LSP/LSA** which consists of a list of names and cost for each of its neighbors.
3. The **LSP/LSA** is transmitted to ***all other routers***. Each router stores the most recently generated **LSP/LSA** from each other router.
 - Link-state flooding: **Sequencing** and **Aging** procedures
 - Each routers store the identical **Link State Database**
4. Each router uses complete information on the network topology to compute the ***shortest path route*** to each destination node.

OSPF(Open Shortest Path First)

41
6

- ▶ OSPF is a standardized Link-State routing protocol. that is used mainly in larger TCP/IP internetworks and within autonomous systems of the Internet.
- ▶ OSPF is more efficient in terms of network overhead than the Routing Information Protocol (RIP), but it is considerably more complex to plan and implement in an enterprise.
- ▶ OSPF will listen to neighbors and gather all link state data available to build a topology map of all available paths in its network and then save the information in its topology database, also known as its Link-State Database (LSDB).
- ▶ Using the information from its topology database. From the information gathered, it will calculate the best shortest path to each reachable subnet/network using an algorithm called Shortest Path First (SPF).
- ▶ OSPF will then construct three tables to store the following information:
- ▶ Neighbor Table: Contains all discovered OSPF neighbors with whom routing information will be interchanged. contains a list of all neighboring routers
- ▶ Topology Table: Contains the entire road map of the network with all available OSPF routes and calculated best and alternative paths.
- ▶ Routing Table: Contain the current working best paths that will be used to forward data traffic between neighbors

OSPF

42
7

- ▶ The default values are 10 seconds for the hello time, and 40 seconds for the dead time. The usual rule of thumb with OSPF is to keep the dead time value four times the hello interval
- ▶ OSPF employs a hierarchical network design using Areas.
- ▶ OSPF will form neighbor relationships with adjacent routers in the same Area.
- ▶ Instead of advertising the distance to connected networks, OSPF advertises the status of directly connected links using Link-State Advertisements (LSAs).

OSPF

- ▶ OSPF sends updates (LSAs) when there is a change to one of its links, and will only send the change in the update. LSAs are additionally refreshed every 30 minutes.
- ▶ OSPF traffic is multicast either to address 224.0.0.5 (all OSPF routers) or 224.0.0.6 (all Designated Routers).
- ▶ OSPF uses the Dijkstra Shortest Path First algorithm to determine the shortest path.
- ▶ OSPF is a classless protocol, and thus supports VLSMs and supports only IP routing.
- ▶ OSPF routes have an administrative distance is 110. OSPF uses cost as its metric, which is computed based on the bandwidth of the link. OSPF has no hop-count limit

Feature

- ▶ Link state protocol.
- ▶ It uses spf(shortest path first) algorithm or Dijkstra algorithm
- ▶ Unlimited hop count
- ▶ Administrative distance is 110.
- ▶ It is a classless routing protocol
- ▶ It support vlsn and cidr
- ▶ It supports only equal cost load balancing.
- ▶ Introduce the concept of area's to ease of management and control traffic.
- ▶ Scales better than distance vector routing protocol.
- ▶ $\text{Metric / Cost} = \text{Reference bandwidth} / \text{Interface bandwidth in bps.}$
- ▶ Cisco uses 100Mbps (108) bandwidth as reference bandwidth. With this bandwidth, our equation would be
- ▶ $\text{Cost} = 108/\text{interface bandwidth in bps}$

BGP(Border Gateway Protocol)

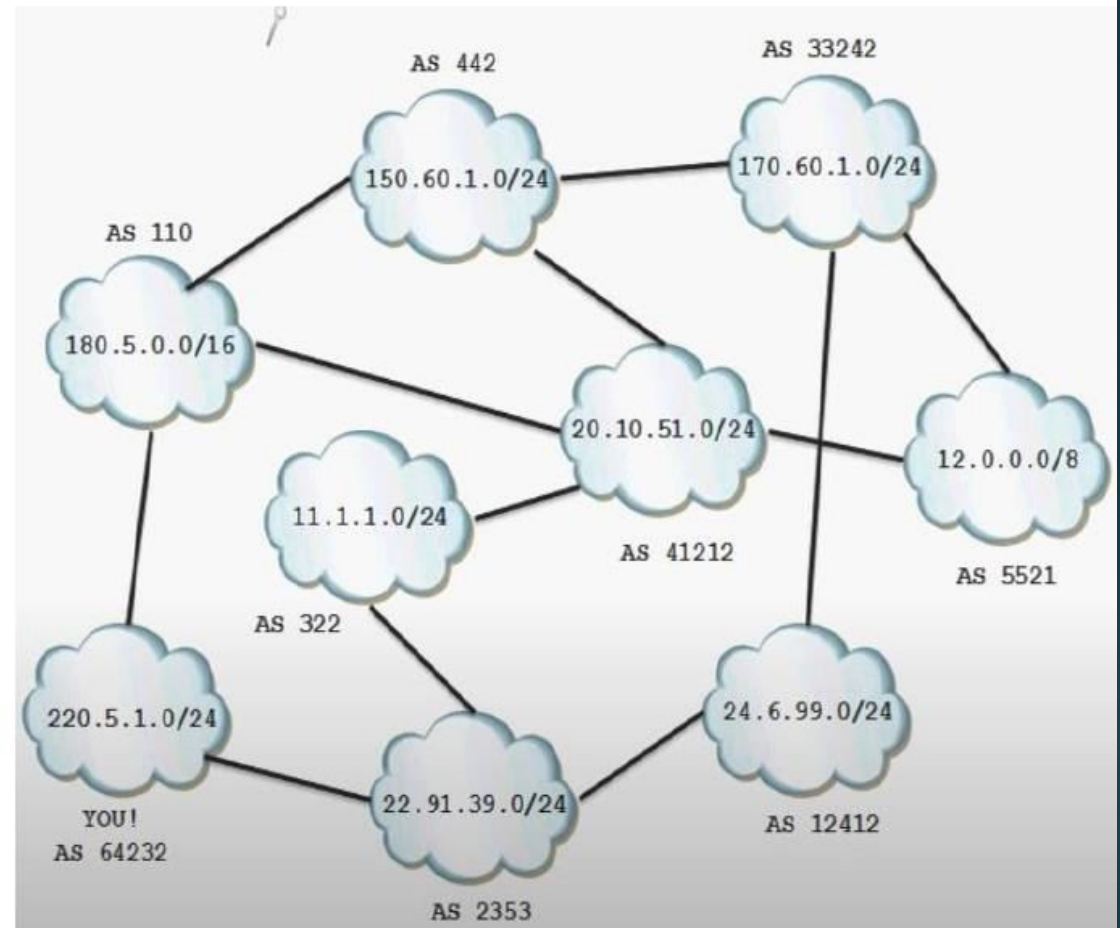
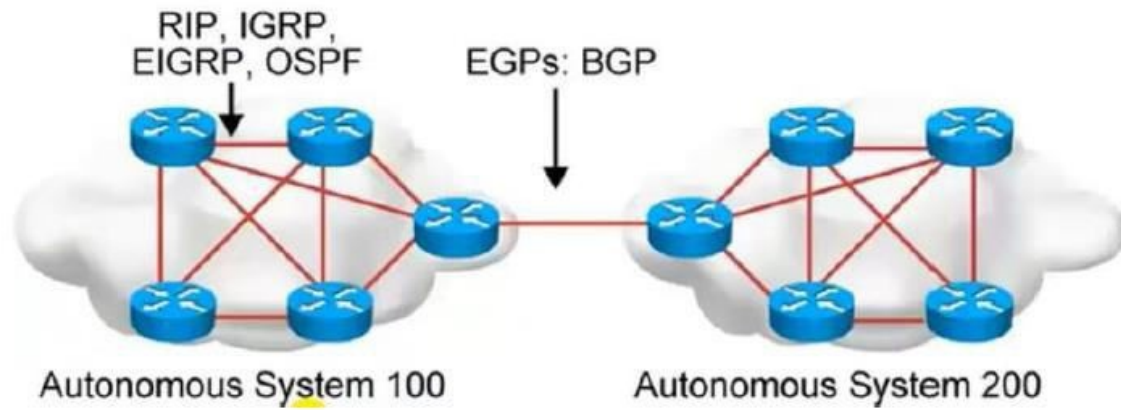
55
0

- ▶ An AS is a collection of networks Under a single technical administration. IGP operates within an AS.
- ▶ BGP protocol is used between AS. which Exchange of loop-free routing information is guaranteed.
- ▶ Exterior gateway routing protocol. Sends updates to manually defined neighbor as unicast
- ▶ BGP is the path-vector protocol that provides routing information for autonomous systems on the Internet via its AS-Path attribute.
- ▶ BGP is the protocol used throughout the Internet to exchange routing information between networks. It is used between AS (known as external BGP), but also as the core routing protocol within large AS (known as internal BGP).
- ▶ Peers that have been manually configured to exchange routing information will form a TCP connection and begin speaking BGP. There is no discovery in BGP.
- ▶ An important aspect of BGP is that the AS-Path itself is an anti-loop mechanism. Routers will not import any routes that contain themselves in the AS-Path.
- ▶ The challenge with BGP is that the protocol does not directly include security mechanisms and is based largely on trust between network operators that they will secure their systems correctly and not send incorrect data.

Summary of Operation

56
1

- ▶ The default value for the hold time is 90seconds, and keep alive should be sent at intervals of one third the hold time (30 seconds).
- ▶ However, Cisco uses defaults of 180 and 60 seconds. So after 180 seconds, router B decides that router A is dead, sends a NOTIFICATION message and tears down the session.
- ▶ Two **hosts form a transport protocol connection between one another**. They exchange messages to open and confirm the connection parameters.
- ▶ The initial data flow is the entire BGP routing table. Incremental updates are sent as the routing tables change. Keep alive messages are sent periodically to ensure the liveness of the connection. Notification messages are sent in response to errors or special conditions.
- ▶ If a connection encounters an error condition, a notification message is sent and the connection is optionally closed.
- ▶ The hosts executing the Border Gateway Protocol need not be routers. A non-routing host could exchange routing information with routers via EGP or even an interior routing protocol. That non-routing host could then use BGP to exchange routing information with a border gateway in another autonomous system.
- ▶ If a particular AS has more than one BGP gateway, then all these gateways should have a consistent view of routing. A consistent view of the interior routes of the autonomous system is provided by the intra-AS routing protocol.



Dijkstra's Algorithm

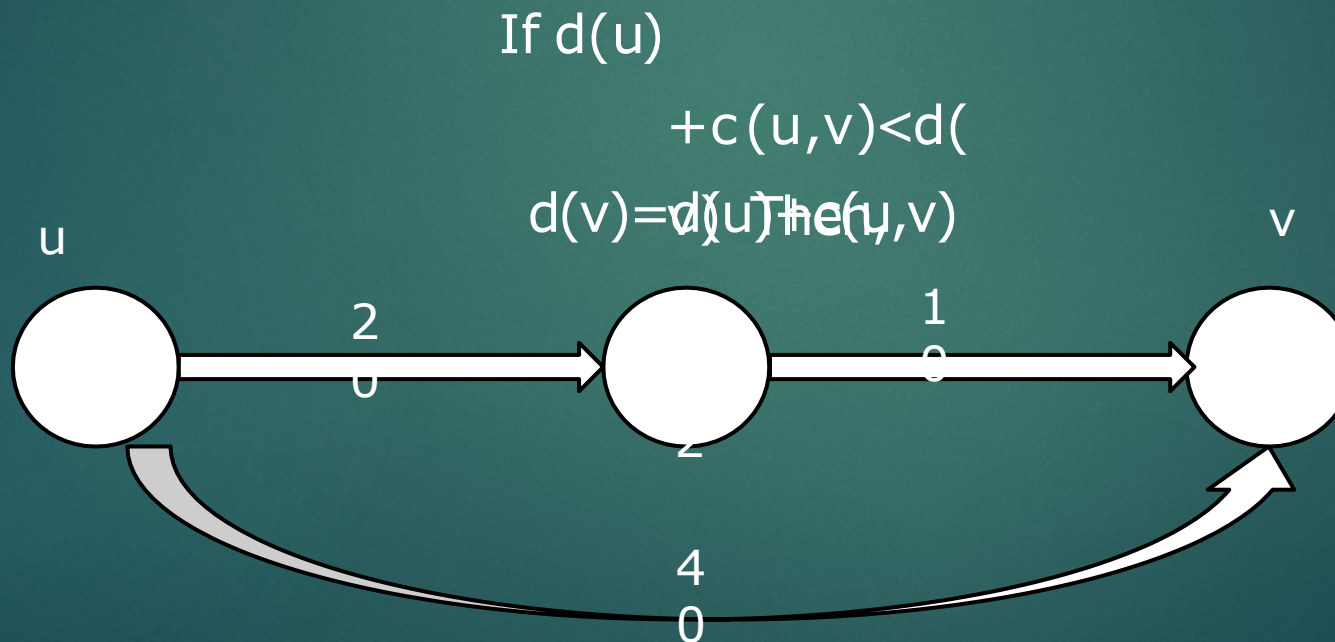
58
3

- ▶ **Dijkstra's algorithm** is an algorithm for finding the shortest paths between nodes in a graph
- ▶ It was conceived by computer scientist Edger W. Dijkstra(Holland) in 1956 and published three years later.
- ▶ Used in GPS to find the shortest path
- ▶ Single source shortest path
- ▶ Dijkstra's Algorithm can only work with graphs that have **positive** weights. This is because, during the process, the weights of the edges have to be added to find the shortest path.

Relaxation

59
4

- The process in Dijkstra's Algorithm refers to the updating the cost of all vertices connected to a vertex v , if those costs would be improved by including the path via v .



Basics of Dijkstra's Algorithm

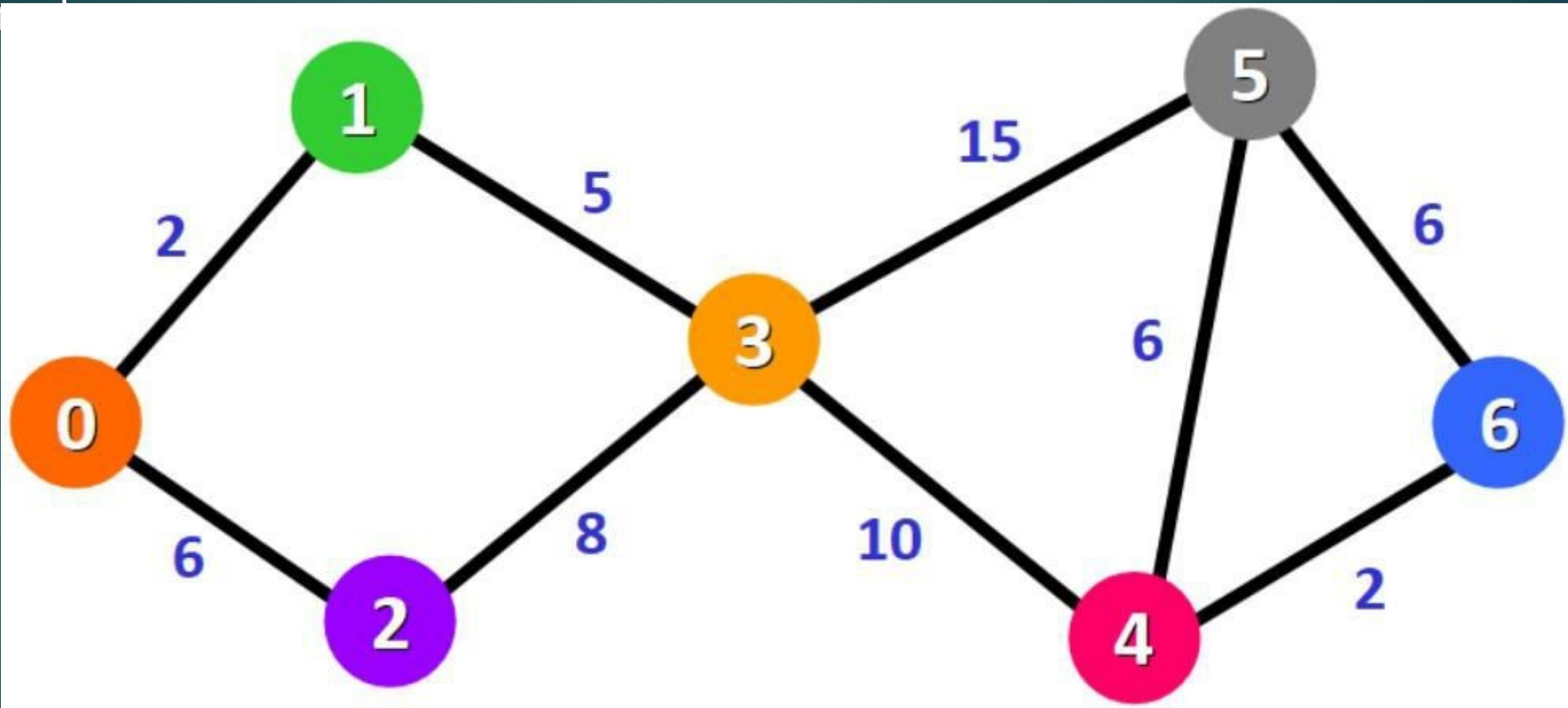
50
5

- Dijkstra's Algorithm basically starts at the node that you choose (the source node) and it analyzes the graph to find the shortest path between that node and all the other nodes in the graph.
- The algorithm keeps track of the currently known shortest distance from each node to the source node and it updates these values if it finds a shorter path.
- Once the algorithm has found the shortest path between the source node and another node, that node is marked as "visited" and added to the path.
- The process continues until all the nodes in the graph have been added to the path. This way, we have a path that connects the source node to all other nodes following the shortest path possible to reach each node.














Example:

561
6

- ▶ Algorithm will generate shortest path from 0 to all the other



Alternative solution can be found in: <https://www.freecodecamp.org/news/dijkstras-shortest-path-algorithm-visual-introduction/>

Source	Destination					
0	1	2	3	4	5	6
	∞	∞	∞	∞	∞	∞
		6	∞	∞	∞	∞
0,1			7	∞	∞	∞
0,1,2				∞	∞	∞
0,1,2,3					22	∞
0,1,2,3,4					22	
0,1,2,3,4,6						

Bellman-Ford Algorithm

53
8

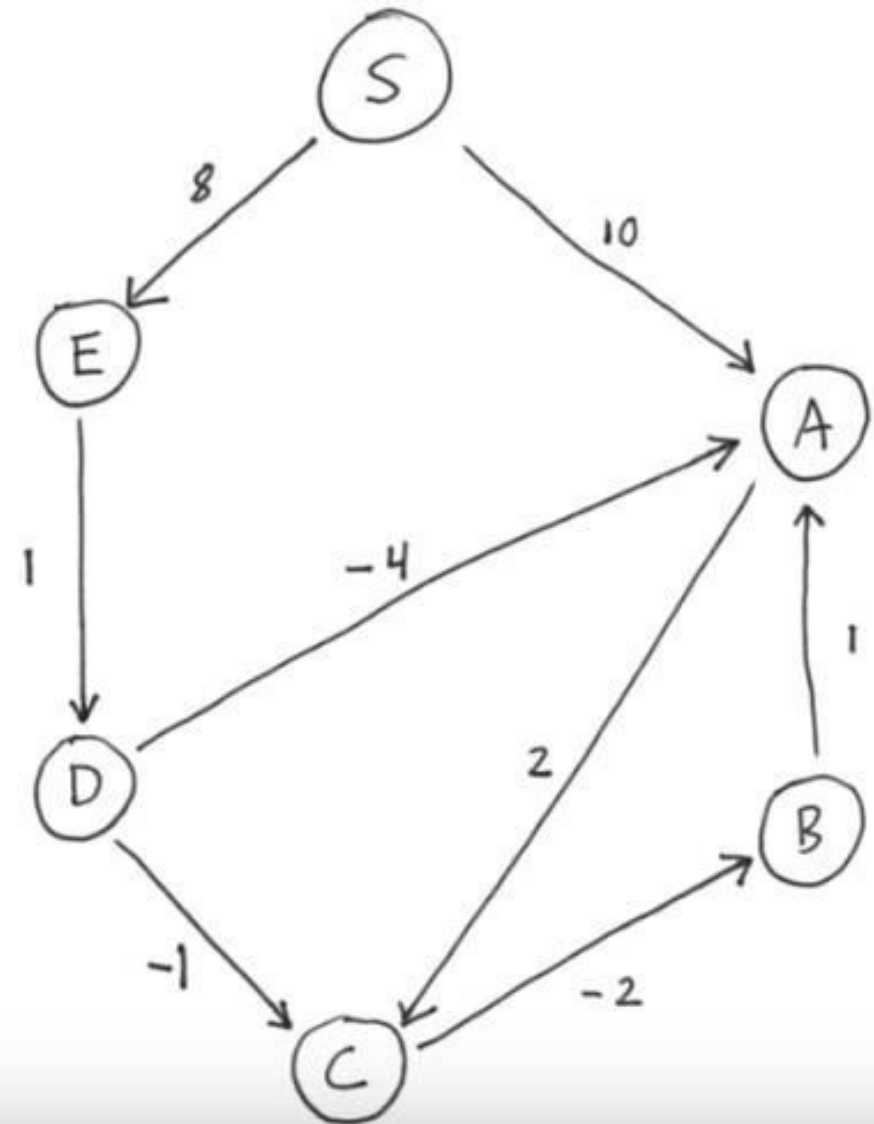
- ▶ computes shortest paths from a single source vertex to all of the other vertices in a weighted digraph.
- ▶ slower than Dijkstra's algorithm for the same problem, but more versatile, as it is capable of handling graphs in which some of the edge weights are negative numbers
- ▶ The algorithm was first proposed by Alfonso Shimbel (1955), but is instead named after Richard Bellman and Lester Ford Jr., who published it in 1958 and 1956, respectively.
- ▶ Edward F. Moore also published a variation of the algorithm in 1959, and for this reason it is also sometimes called the **Bellman–Ford–Moore algorithm**.
- ▶ You have to relax every edge $v-1$ number of times where v is the number of vertices.

Bellman Ford Algorithm

54

- Lets consider S be the source First Iteration

S	A	B	C	D	E
0	∞	∞	∞	∞	∞
0	10	∞	∞	∞	8
0	10	∞	12	9	8
0	10	10	12	9	8



Bellman Ford Algorithm

65

► Second Iteration

S	A	B	C	D	E
0	5	10	8	9	8

► Third Iteration

S	A	B	C	D	E
0	5	5	7	9	8

► Fourth Iteration

S	A	B	C	D	E
0	5	5	7	9	8

